Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A network comprising:

IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for encrypting and authenticating communications via the Internet between two different centers; and

an IPsec setting apparatus, which manages IPsec settings of the IPsec processing apparatuses,

wherein in response to receiving a request from a first IP processing apparatus to communicate with a second IPsec processing apparatus, the IPsec setting apparatus transmits a request to the second IPsec processing apparatus and upon receiving a reply to the request from the second IPsec processing apparatus the IPsec setting apparatus transmits a common encryption key to the first and second IPsec process apparatuses to be used to encrypt and authenticate IPsec communications between the first and second process apparatuses;

wherein said IPsec setting apparatus generates SA (Security Association) parameters, to be used in the IPsec communication between the first and the second IPsec processing apparatuses, based on the contents of the request message and contents of IPsec policies stored by the IPsec setting apparatus;

wherein said IPsec setting apparatus sends a distribution message including the policies of said IPsec and the SA parameters in response to the request message; and

wherein the IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires,

wherein said IPsec setting apparatus generates the common encryption key to be used in encryption and authentication of the IPsec communications between the first IPsec processing apparatus and the second IPsec processing apparatus and transmits the generated common encryption key to the IPsec processing apparatus.

2. (Canceled)

3. (Previously Presented) The network of claim 1,

wherein the second IPsec processing apparatus transmits a request for the communication message as a reply to the request received from the IPsec setting apparatus.

4. (Previously Presented) The network of claim 1,

wherein when there is no response from the second IPsec to the request from the IPsec setting apparatus the IPsec setting apparatus notifies the first IPsec processing apparatus that there is no response from said second IPsec processing apparatus.

5. – 7. (Canceled)

8. (Currently Amended) An IPsec setting apparatus managing IPsec setting of IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing communication via the Internet between two different centers,

wherein said IPsec setting apparatus manages IPsec policies applied among the IPsec processing apparatuses,

wherein said IPsec setting apparatus specifies the IPsec policies to be applied between a first IPsec processing apparatus, requesting communication with a second IPsec processing apparatus, and the second IPsec processing apparatus, based upon contents of the request to the IPsec setting apparatus from the first IPsec processing apparatus for communication with the second IPsec processing apparatus, said IPsec setting apparatus generating a common encryption key to be used in encryption and authentication of IPsec communication and distributes the generated common encryption key to the first and second IPsec processing apparatuses;

wherein said IPsec setting apparatus generates SA (Security Association) parameters used in the IPsec communication between the first IPsec processing apparatus and the second

IPsec processing apparatus based upon the contents of the request message and contents of the IPsec policies stored by the IPsec setting apparatus;

wherein said IPsec setting apparatus simultaneously transmits to the first IPsec processing apparatus and to the second IPsec processing apparatus a message including at least the policies and the SA parameters for IPsec communication between the first IPsec processing apparatus and the second IPsec processing apparatus in response to the request message; and

wherein the first IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires,

wherein said IPsec setting apparatus generates the common encryption key to be used in encryption and authentication of the IPsec communications between the first IPsec processing apparatus and the second IPsec processing apparatus and transmits the generated common encryption key to the IPsec processing apparatus.

9. (Canceled)

10. (Previously Presented) The IPsec setting apparatus of claim 8,

wherein said IPsec setting apparatus upon receiving the request message from the first IPsec processing apparatus, transmits a request startup message to the second IPsec processing apparatus, which is an opposite party of communication of the first IPsec processing apparatus which has transmitted the request message, in order to cause the second IPsec processing apparatus to transmit a request message for the communication.

11. (Previously Presented) The IPsec setting server apparatus of claim 10,

wherein the IPsec setting apparatus, when there is no response to the request startup message from the second IPsec processing apparatus, notifies the first IPsec processing apparatus which has transmitted the request message that there is no response from the second IPsec processing apparatus of the opposite party of communication.

12. – 14. (Canceled)

15. (Currently Amended) An IPsec processing apparatus using an IPsec (Internet Protocol security protocol) on the Internet,

wherein said IPsec processing apparatus receives from an IPsec setting apparatus managing communication a packet containing the IPsec to be applied to communications with another IPsec processing apparatus, determines whether or not to request from the IPsec setting apparatus a setting for IPsec communication, and wherein the IPsec processing apparatus transmits a request for communication with the other IPsec processing apparatus to the IPsec setting apparatus in order to receive from the IPsec setting apparatus a setting for IPsec communication, the IPsec processing apparatus received from the IPsec setting apparatus a common encryption key to be used in encryption and authentication of said IPsec communication; and

wherein said IPsec processing apparatus includes means for setting an SPD (Security Processing Database), in which policies for applying said IPsec is recorded, and an SAD (Security Association Database), in which an SA (security Association) necessary for subjecting an individual communication to the IPsec processing is stored, based upon a message received from the IPsec setting apparatus; and

wherein said IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires,

wherein said IPsec processing apparatus receives the common encryption key generated by said IPsec setting apparatus to be used in encryption and authentication of the IPsec communications between said IPsec processing apparatus and the other IPsec processing apparatus.

16. (Canceled)

17. (Previously Presented) The IPsec processing apparatus of claim 15,

wherein, upon receiving a request startup message from an IPsec setting apparatus the IPsec processing apparatus transmits a request for communication with another IPsec processing apparatus to the IPsec setting apparatus.

18. -20. (Canceled)

21. (Currently Amended) An IPsec setting method for a network comprising:

receiving from a first IPsec processing apparatus a request for communication with a second IPsec processing apparatus;

in response to the received request, sending a request to the second IPsec processing apparatus,

receiving a reply to the sent request from the second IPsec processing apparatus,

in response to the reply from the second IPsec processing apparatus, retrieving IPsec policy rules from memory based on the content of the request from the first IPsec processing apparatus and the retrieved policy rules, generating a common encryption key to be used in encryption and authentication of IPsec communication between the first and second IPsec processing apparatuses;

transmitting the generated common encryption key to first and second IPsec processing apparatuses;

in response to a reply from the second IPsec processing apparatus, generating SA (Security Association) parameters to be used in the IPsec communication between the first and second IPsec processing apparatuses based on contents of the request from the first IPsec processing apparatus message and the retrieved policy rules;

transmitting a distribution message including at least the retrieved policies and generated SA parameters in response to receiving the request; and

receiving a second request from the first IPsec processing apparatus for communication with the second IPsec processing apparatus before a term of the validity of an SA (Security Association) parameter expires, and in response, generating and transmitting new IPsec setting to the first and second IPsec processing apparatuses.

wherein the common encryption key is generated to be used in encryption and authentication of the IPsec communications between the first IPsec processing apparatus and the second IPsec processing apparatus; and

transmitting the generated common encryption key from said IPsec setting apparatus to the IPsec processing apparatus.

22. (Canceled)

23. (Previously Presented) The IPsec setting method of claim 21,

wherein the request sent to the second IPsec is a startup message and the reply received from the second IPsec is a request for the communication.

24. (Previously Presented) The IPsec setting method of claim 21,

wherein when there is no reply to the request sent to the second IPsec processing apparatus, notifying the first IPsec processing apparatus that there is no response from the second IPsec processing apparatus.

25. -27. (Canceled)

28. (Previously Presented) The IPsec setting method of claim 21,

further compromising, upon receiving at one of the first and second IPsec processing apparatuses a communication to which an IPsec should be applied, the IPsec processing apparatus determines whether or not to request an IPsec setting from an IPsec setting apparatus.

29. (Previously Presented) The IPsec setting method of claim 21,

wherein the first IPsec processing apparatus transmits a request for communication with the second IPsec processing apparatus to an IPsec setting apparatus in order to acquire a setting for the IPsec to be used during the communication.

30. (Previously Presented) The IPsec setting method of claim 21,

wherein the IPsec processing apparatuses store the retrieved policies transmitted in the distribution message in a respective SPD, and store the SA parameters transmitted in the distribution message in a respective SAD.

31. (Canceled).

32. (Canceled)

33. (Previously Presented) The network of claim 1 wherein the common encryption key transmitted by the IPsec setting apparatus in response to the request depends on an address of the first IPsec processing apparatus making the request.

34. (Previously Presented) The network of claim 1 wherein the common encryption key transmitted by the IPsec setting apparatus in response to the request depends on an address of the second IPsec processing apparatus for which communication is requested.

35. (Previously Presented) The network of claim 1 wherein the common encryption key transmitted by the IPsec setting apparatus in response to the request depends on addresses of the first IPsec processing apparatus making the request and the second IPsec processing apparatus for which communication is requested.

36. (Previously Presented) The network of claim 1 wherein all communications between the first IPsec processing apparatus and the IPsec setting apparatus are encrypted, and all communications between the second IPsec processing apparatus and the IPsec setting apparatus are encrypted.